



Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada



s.15(1)
s.21(1)(a)
s.21(1)(b)
s.23

SECRET
Cerrid # 848832
CCM# 11-03360

14 November 2011

MEMORANDUM FOR THE CHIEF

Updated Collection and Use of Metadata Ministerial Directive

(For Approval)

Summary

- This Memorandum seeks your approval for the proposed changes to the 2005 Collection and Use of Metadata Ministerial Directive.
- The updated MD will enable SIGINT to
- DLS, SIGINT were consulted in the development of the proposed changes to the MD.
- Should you approve the changes to this Ministerial Directive, it is recommended that it be presented to the Minister of National Defence at the 21 November 2011 briefing.

Background

- The current Collection and Use of Metadata Ministerial Directive allows SIGINT to metadata foreign intelligence collection activities
- SIGINT must follow procedures
-
-

SECRET

Cerrid # 848832
CCM# 11-03360

s.15(1)

s.21(1)(a)

s.21(1)(b)

- CSEC's reporting protocols and procedures on disclosure will continue to protect the privacy of Canadians.

Recommendation

- It is recommended that you approve the proposed changes to the updated Ministerial Directive on Metadata and that it be presented to the Minister of National Defence for approval.

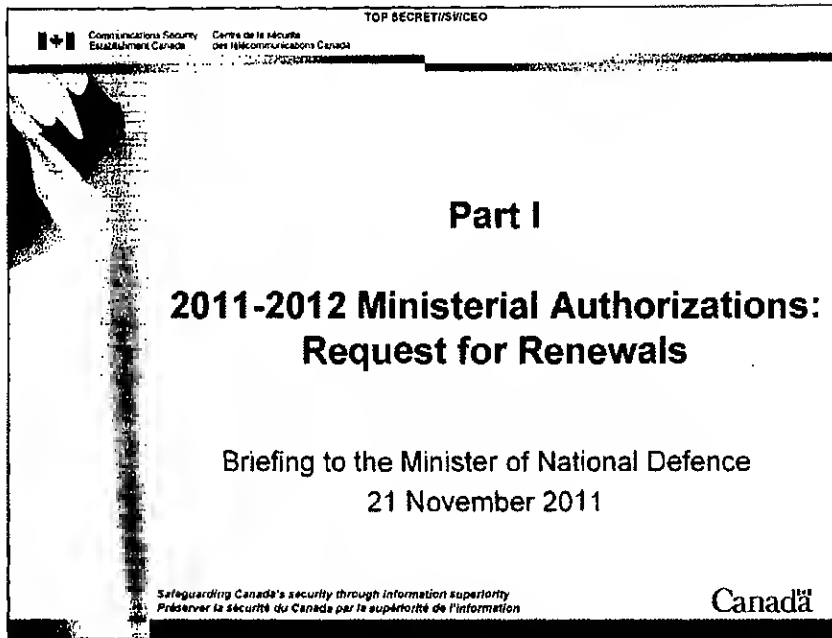
Next Steps

- If you approve, this Ministerial Directive will be incorporated into the 21 November 2011 briefing package for approval by the Minister.
- Speaking notes and an additional slide for presentation to the Minister have been developed and are attached for your review.
- You are meeting with the NSA on 15 November 2011. It is proposed that you brief the NSA on your intentions regarding this Ministerial Directive. The attached slide and speaking notes which have been added to the Minister's package will support your meeting with the NSA.
- As per established practice, DGPC will share the proposed changes to the Ministerial Directive with PCO S&I in advance of your meeting with the NSA.


Kathy Thompson
Director-General
Policy and Communications

I approve:

John Adams
Chief



s.15(1)
s.21(1)(a)
s.21(1)(b)


 Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

TOP SECRET//SI//CEO

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

TOP SECRET//SI//CEO

Ministerial Authorizations: Overview

- MAs authorize CSEC to engage in activities which risk incidental interception of private communications, which would otherwise be considered a violation of the *Criminal Code*
- The MA regime enables CSEC to conduct operations consistent with its mandate and Government of Canada intelligence priorities
- Protection of Canadians' privacy is a key element
- All MAs are reviewed by the CSE Commissioner (OCSEC)
- To date, OCSEC has found CSEC activities reviewed to be lawful

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

Under section 273.65 (2) of the *NDA*, the Minister of National Defence may authorize CSEC to engage in foreign intelligence collection activities which may result in the incidental interception of private communications, if the Minister is satisfied that:

- the interception will be directed at foreign entities located outside Canada;
- the information to be obtained could not reasonably be obtained by other means;
- the expected foreign intelligence value of the information that would be derived from the interception justifies it; and
- satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence, or security.

Under 273.65 (4) of the *NDA*, the Minister of National Defence may authorize CSEC to engage in computer system or network protection activities for the Government of Canada which may result in the incidental interception of private communications, if the Minister is satisfied that:

- the interception is necessary to identify, isolate or prevent harm to Government of Canada computer systems and networks;
- the information to be obtained could not reasonably be obtained by other means;
- satisfactory measures are in place to ensure that only information that is essential to identify, isolate or prevent harm to Government of Canada computer systems or networks will be used or retained; and
- satisfactory measures are in place to protect the privacy of Canadians in the use or retention of that information.

Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

CSEC is requesting the following SIGINT MAs :

- s.15(1)**

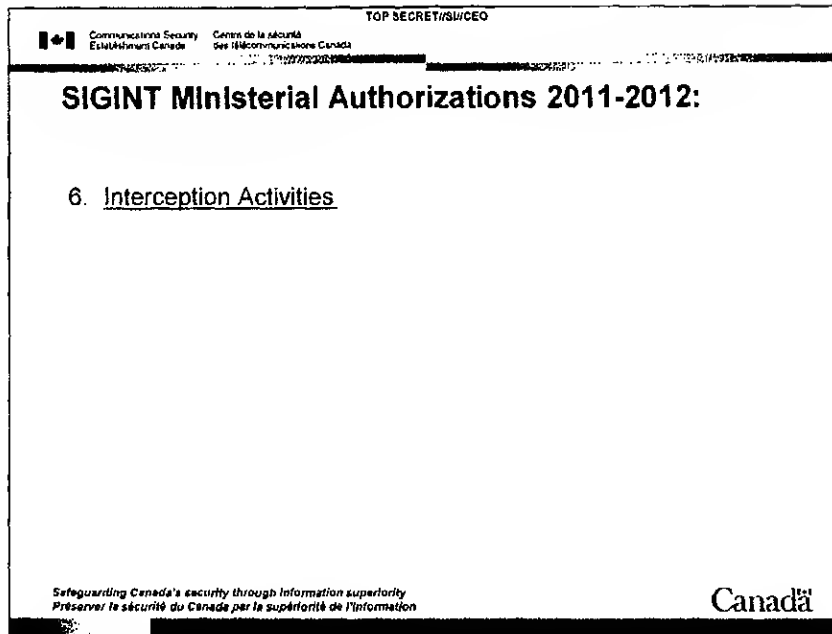
s.21(1)(a)

s.21(1)(b)

**Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information**

Canadă

s.15(1)
s.21(1)(a)
s.21(1)(b)



Interception Activities


- There are now six SIGINT MAs,

s.15(1)

s.21(1)(a)

s.21(1)(b)

s.15(1)
s.21(1)(a)
s.21(1)(b)

 Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada


TOP SECRET//SI//CEO

Information Protection


Ministerial Authorizations: 2011-12

CSEC is requesting the following Information Protection MAs:

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information



s.15(1)
s.21(1)(a)
s.21(1)(b)



Communications Security
Establishment Canada

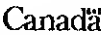
Centre de la sécurité
des télécommunications Canada

TDP SECRET//SI//C EO

Minor Changes


- Minor changes include:
 -
 -
- Scope of MAs remains unchanged

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information



However, there are minor changes worth noting:


- This is consistent with direction to the Canadian S&I community in this year's Intelligence Priorities, in the Ministerial Directive you provided to CSEC,


TOP SECRET//SI//CEO	
Communications Security Establishment Canada	Centre de la sécurité des télécommunications Canada
Proposed Change: MA	
<ul style="list-style-type: none">By signing the MA you will signal concurrence with this change	
<small>Safeguarding Canada's security through information superiority Préserver la sécurité du Canada par la supériorité de l'information</small>	
	

s.15(1)
s.21(1)(a)
s.21(1)(b)
s.23

The notable change to the MAs this year is:

s.15(1)
s.21(1)(a)
s.21(1)(b)

 Communications Security
Establishment Canada

 Centre de la sécurité
des télécommunications Canada

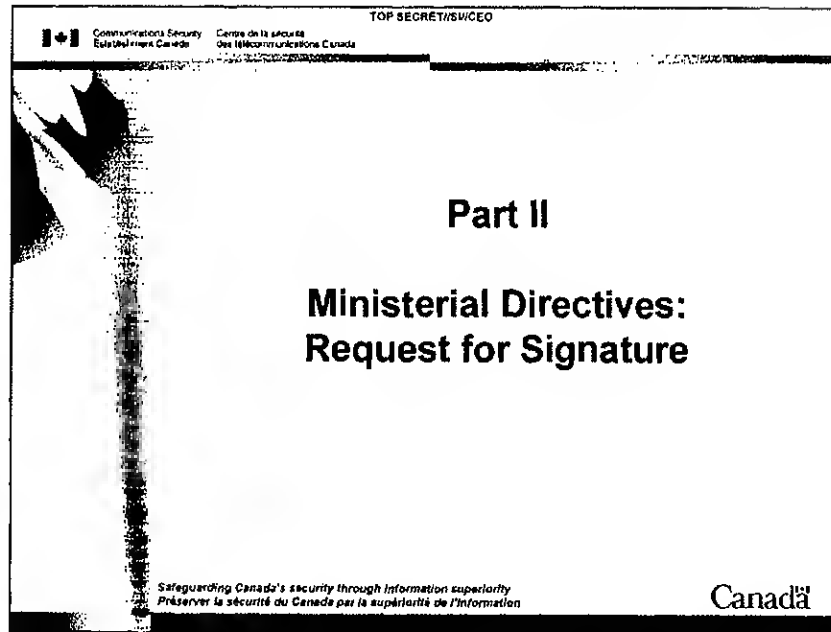
TOP SECRET//SI//CEO

Recommendation

- The National Security Advisor concurs with CSEC's recommendation that the Minister of National Defence approve the MA package
- The Deputy Minister of National Defence has been informed of this recommendation
- It is recommended you approve the 2011-2012 CSEC MA request

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information





s.15(1)

s.21(1)(a)

s.21(1)(b)

TOP SECRET//SI//CEO

Communications Security Establishment Canada / Centre de la sécurité des télécommunications Canada

Ministerial Directives:

- Four Ministerial Directives (MDs) related to CSEC require your signature.

The MDs are:


1. MD
2. MD
3. MD
4. MD

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

- These MDs are directly related to the Ministerial Authorization

- The MDs are renewed annually in conjunction with the Ministerial Authorization package.

**Communications Security
Establishment Canada**

**Centre de la sécurité
des télécommunications Canada**

TOP SECRET//SI//CEO

MD on Assistance to Federal Law Enforcement and Security Agencies

- Replaces 2001 Support to Law Enforcement and National Security Agencies MD, with a focus on CSEC assistance mandate (Mandate C)
- Responds to Commissioner's recommendation to update pre-legislation MDs, and consistent with legislation, original direction and operational practice
- As a priority, all Operational Policies will be updated before new elements of this MD are operationalized
- CSEC will return to you should there be any issues with operationalizing the MD
- CSEC will continue to review other pre-legislation MDs

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

- In addition to our regular package of renewals there are three additional MDs ready for you signature.
- The first responds to a CSE Commissioner recommendation to update the MDs that predate the establishment of CSEC legislation.
- The first priority is the 2001MD that outlines our support to RCMP, CSIS and other law enforcement and security agencies under lawful access.
- The new MD will replace the 2001 MD and is focused on our legislated mandate for assistance to federal law enforcement and security agencies.
- The MD is consistent with our legislation and the original direction with some added clarifications that are consistent with our current operational practice.
- CSEC will continue to review other pre-legislation MDs (on Privacy and Accountability) to assess whether any other updates are required.

TOP SECRET//SI//CEO

Communications Security Establishment Canada / Centre de la sécurité des télécommunications Canada

MD on Framework


-
-
- CSEC MD recognizes CSEC's role as a foreign signal intelligence agency, and maintains long-standing alliance with Five-Eyes partners
-
- With your approval, and as a priority, CSEC will finalize and codify these interim measures to support the MD

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

s.15(1)
s.21(1)(a)
s.21(1)(b)
s.23
s.69(1)(g)re:c

- For CSEC, the MD is tailored to specifically reflect our foreign signals intelligence role.


 Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

TOP SECRET//SI//RCO

MD on Collection and Use of Metadata

- Proposed changes to 2005 MD reflect
- The updated MD will enable SIGINT to
- CSEC's reporting structure and disclosure procedures remain adequate to protect the privacy of Canadians
- As a priority, all relevant Operational Policies will be updated before this MD is operationalized
- CSEC will return to you should there be any issues with operationalizing the MD

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information




s.15(1)
s.21(1)(a)
s.21(1)(b)


- I am seeking your approval for an updated *MD on Collection and Use of Metadata*.
- As you know, the current Metadata MD has been in place since 2005.
- Metadata is information associated with a telecommunication and not a communication.

- The existing MD allows SIGINT to :

- Consequently, does not represent a reasonable threshold for privacy concerns and therefore current privacy protection measures are adequate.
- CSEC's reporting protocols and procedures will continue to protect the privacy of Canadians.

s.15(1)

 Communications Security Establishment Canada

 Centre de la sécurité des télécommunications Canada

TOP SECRET//SI//CEO

Recommendation

- The National Security Advisor concurs with CSEC's recommendation that the Minister of National Defence approve the following Ministerial Directives:
 - ~ Four MDs;
 - ~ Updated Assistance MD;
 - ~ MD; and
 - ~ Metadata MD.
- It is recommended you approve the seven proposed Ministerial Directives

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada



Communications Security Centre de la sécurité
Establishment Canada des télécommunications Canada



s.15(1)
s.21(1)(a)
s.21(1)(b)

SECRET
CERRID # 851237
CCM#11-03394

NOV 17 2011

MEMORANDUM FOR THE MINISTER OF NATIONAL DEFENCE

Collection and Use of Metadata Ministerial Directive

(For Approval)

Summary

- This Memorandum seeks your approval of proposed changes to the 2005 Collection and Use of Metadata Ministerial Directive.
- The updated MD will enable CSEC Signals Intelligence (SIGINT) to
- It is recommended that you approve the attached Collection and Use of Metadata Ministerial Directive.

Background

- Metadata is information associated with a telecommunication and not a communication.
- The current Collection and Use of Metadata Ministerial Directive allows SIGINT to metadata from its foreign intelligence collection activities
- SIGINT must follow procedures

Canada

000020

A0362855_1-000020

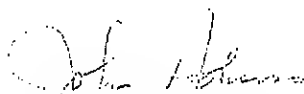
~~SECRET~~
CERRID # 851237
CCM# 11-03394

s.15(1)
s.21(1)(a)
s.21(1)(b)
s.23

- CSEC's reporting protocols and procedures on disclosure will continue to protect the privacy of Canadians.

Recommendation

- It is recommended that you approve the revised Collection and Use of Metadata Ministerial Directive.


John Adams
Chief

I concur with this recommendation:


Stephen Rigby
National Security Advisor to the Prime Minister

cc. Robert Fonberg
Deputy Minister of National Defence



National
Defence

Défense
nationale

TOP SECRET//SI

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

s.15(1)

To: Chief, Communications Security Establishment

**MINISTERIAL DIRECTIVE
COMMUNICATIONS SECURITY ESTABLISHMENT
COLLECTION AND USE OF METADATA**

1. This Directive is issued under my authority pursuant to subsection 273.62 (3) of the *National Defence Act*.
2. For the purpose of the CSE's foreign intelligence acquisition programs pursuant to paragraph 273.64 (1) (a) of the *National Defence Act*:
 - a) "**metadata**" means information associated with a telecommunication
 - b)
 - c)
3. This Ministerial Directive relates to the activities carried out pursuant to paragraph 273.64 (1) (a) of the *National Defence Act* (CSE's foreign intelligence acquisition programs). CSE will collect and use metadata under foreign intelligence acquisition programs according to principles enunciated in this Ministerial Directive. Any amendment to this Ministerial Directive will require my personal approval.

Canada

TOP SECRET//SI

TOP SECRET//SI

s.15(1)

4. Metadata acquired pursuant to its foreign intelligence acquisition programs will be subject to CSE's existing procedures to protect the privacy of Canadians.
5. In the fulfillment of its mandate as set out in paragraph 273.64 (1) (a) of the *National Defence Act*, CSE may metadata acquired in the execution of its foreign intelligence acquisition programs
6. CSE will metadata, acquired through its foreign intelligence acquisition programs to maximize its mandate activities as set out in the *National Defence Act*, will be subject to strict conditions to protect the privacy of Canadians, consistent with these standards governing CSE's other programs.
7. CSE must take the following steps to protect the privacy of Canadians:
 - (1)
 - (2)
 - (3)
 - (4)
 - (5) Any use or retention of this metadata for the purposes set out in paragraph 273.64 (1) (b) will continue to be handled in accordance with existing policy and procedures related to the protection of the privacy of Canadians.
8. The metadata acquired in the execution of the CSE's foreign intelligence acquisition programs shall be used strictly for:
 - a)

TOP SECRET//SI

s.15(1)

b)

c)

9. The metadata acquired in the execution of CSE foreign intelligence acquisition programs
10. Activities undertaken pursuant to this Ministerial Directive are subject to review by the CSE Commissioner to ensure they are in compliance with the law.
11. This Ministerial Directive replaces the Ministerial Directive Communications Security Establishment Collection and Use of Metadata, signed by the Minister of National Defence on March 9, 2005.
12. This Ministerial Directive comes into force on the date it is signed.

Dated at Ottawa, Ont this 21st day of November, 2011.



The Honourable Peter MacKay, P.C., M.P.
Minister of National Defence

cc. National Security Advisor, Privy Council Office
Deputy Minister of National Defence



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

P.O. Box 9703
Terminal
Ottawa, Canada
K1G 3Z4

C.P. 9703
Terminus
Ottawa, Canada
K1G 3Z4

TOP SECRET//SI//
Canadian Eyes Only

s.15(1)

Your File Votre référence

Our file Notre référence

CCSE/155-11
#816595

December 13, 2011

The Honourable Robert Décary, QC
Communications Security Establishment Commissioner
90 Sparks Street, Suite 730
P.O. Box 1984, Postal Station "B"
Ottawa, Ontario
K1P 5B4

Dear Commissioner:

I would like to advise you that the Minister issued eight Ministerial Authorizations and seven Ministerial Directives on 21 November 2011, which came into effect on 1 December 2011. Please find enclosed copies of the signed versions of the following Ministerial Authorizations issued pursuant to section 273.65 of the *National Defence Act*:

- Interception
-
- CSE Interception Activities
- Interception
- Interception Activities Conducted in Support of the Government of Canada Mission in Afghanistan
-
-
-

Additionally, the following seven Ministerial Directives were issued pursuant to subsection 273.62(3) of the *National Defence Act*:

- Ministerial Directive: Assistance to Federal Law Enforcement and Security Agencies
- Ministerial Directive: Framework

Canada

000025

A0362857_1-000025

- 2 -

TOP SECRET//SI//
Canadian Eyes Only

- Ministerial Directive: Collection and Use of Metadata
- Ministerial Directive:
- Ministerial Directive:
- Ministerial Directive:
- Ministerial Directive:

s.15(1)

s.21(1)(a)

s.21(1)(b)

Sincerely,

John Adams
Chief

Enclosures

000026

A0362857_2-000026

ADVICE FOR THE MINISTER

CSEC ISSUES

ISSUE: Why is the government putting national security at risk with the LTA project by hiring contractors to work at CSEC? Why is the government allowing the loss of more than 90 Public Service positions by hiring contractors rather than full-time public servants? Why was Plenary Properties, a foreign-owned Australian company, selected to construct the new facility for Canada's most secret intelligence organization? What is the government doing to ensure that Government of Canada computers and information are protected from cyber-attacks?

IF PRESSED ON IMPACT OF LONG-TERM ACCOMMODATION (LTA) PROJECT ON NATIONAL SECURITY

- National security is in no way at risk as a result of this project. All CSEC staff, including contractors, are subject to the appropriate security screening process and clearance level.
- Any private contractor hired for the new facility who will have access to sensitive information will be designated as a Person Permanently Bound to Secrecy and subject to the *Security of Information Act* in the same manner as CSEC employees.
- Contractors have been employed by CSEC for many years. At any given time, there are more than 100 contractors working at CSEC. All contractors have the appropriate security clearances, have sworn the appropriate oaths of secrecy and have signed the appropriate documents to be employed by CSEC.

IF PRESSED ON IMPACT OF LTA PROJECT ON CSEC EMPLOYEES' JOB SECURITY

- No CSEC employee will lose employment as a result of this public private partnership.
- The Chief of CSEC is fully committed to ensuring that any employee whose job is affected by the move to the new facility four to five years from now is guaranteed another position at CSEC or elsewhere within the federal public service.
- In fact, this project will create jobs – approximately 4000 construction jobs will be created as a result of this project.

**IF PRESSED ON PLENARY GROUP (CANADA) AND CANADIAN
BUILDER PCL CONSTRUCTION**

- Plenary Group, the Plenary Properties consortium lead, is a Canadian company with offices in Toronto, Vancouver and Edmonton.
- Plenary Group has an Australian sister company with industry-leading experience in Australian-based public-private-partnership projects; however, this company is not involved in the project.
- Plenary Group has a proven track record of creating Canadian jobs. This project is expected to generate upwards of 4,000 jobs for Canadians, 99 percent of which are expected to be Canadian.
- With a project of this size and complexity, it is only reasonable to expect that the consortium would be Canadian-led and multinational in nature.

**IF PRESSED ON CYBER COMPROMISES OF GOVERNMENT OF
CANADA COMPUTER SYSTEMS**

- CSEC provides the Government of Canada, departments and agencies advice, guidance and services on the protection of electronic information and infrastructures.
- CSEC is recognized as a key partner in Canada's *Cyber Security Strategy*.
- While the Government does not comment on the specific operational details of security-related incidents, I can assure you that CSEC continues to work with departments in addressing unauthorized attempts to access their networks.

IF PRESSED ON OCSEC ANNUAL REPORT, 2010-11

- As the Communications Security Establishment Commissioner confirmed in his annual report, CSE activities that he examined this past year were all in compliance with the law, ministerial requirements, and CSE policies and procedures.
- The Commissioner made a small number of recommendations, and expressed satisfaction that CSEC addressed deficiencies identified in previous annual reports.

**IF PRESSED ON CSEC COLLECTION OF CANADIANS' PERSONAL
INFORMATION**

- CSEC does not target the communications of Canadians anywhere and has legislative measures in place for the protection of the privacy of Canadians.
- As the CSE Commissioner has noted in his 2010-2011 report, the focus of CSEC activity is foreign intelligence.
- The CSE Commissioner highlighted that all reviewed CSEC activities were authorized and carried-out in accordance with the law, ministerial requirements and CSEC's policies and procedures.
- In his report, the Commissioner highlights the degree of transparency and cooperation displayed by CSEC, as well as CSEC's genuine concern for protecting the privacy of Canadians.

BACKGROUND

PLENARY GROUP CONSORTIUM

- The consortium includes 11 companies, 7 of which are wholly Canadian and 4 are incorporated in Canada.
- Plenary Properties earned the highest score in all sections of the evaluation criteria.
- Plenary Properties received a bond rating of A, the highest grade of any PPP ever awarded in Canada.

CYBER SECURITY

- The Communications Security Establishment Canada has a mandate to provide advice, guidance, and services to help ensure the protection of electronic information and information infrastructures of importance to the Government of Canada.
- In October 2010, the Government released *Canada's Cyber Security Strategy*. The Strategy has three pillars:
 - o Secure government systems;
 - o Partnering to secure vital cyber systems outside the federal government; and,
 - o Helping Canadians to be secure online.
- CSEC is a key player in the pillar to Secure Government Systems.
- Budget 2010 included an investment of \$90 million over five years to implement the Strategy.
- The Strategy states that with its unique mandate and knowledge, CSEC will enhance its capacity to detect and discover threats, provide foreign intelligence and cyber security services, and respond to cyber threats and attacks against Government networks and information technology systems.
- The Strategy states that Public Safety will coordinate implementation of the Strategy.

OCSEC ANNUAL REPORT 2010-11

- The Commissioner's 2010-2011 Annual Report noted that "when other means have been exhausted, CSEC may use information about Canadians when it has reasonable grounds to believe that using this information may assist in identifying and obtaining foreign intelligence."
- Citing the above, a 29 July 2011 Globe and Mail article referred to CSEC using "information about Canadians... in identifying and obtaining foreign intelligence."
- The story noted these activities were halted and resumed after "major changes."
- The suspension was initiated by the Chief of CSEC, in order to make absolutely certain that the activities in question were compliant with Canadian privacy laws as well as with CSEC's own policies and procedures.
- In consultation with the Department of Justice an internal review determined that these activities were indeed in compliance with the law but it was felt that certain CSEC policies should be clarified. This was done and CSEC resumed these activities.
- As an independent organization, the Office of the Communications Security Establishment Commissioner can review all activities carried out by CSEC for lawfulness, and must review all activities carried out under Ministerial Authorizations.

MEDIA BACKGROUND

- On 26 Sep 11, media reported that the Government was warned prior to the cyber compromises of January 2011 that a hacking attempt could possibly occur. According to this reporting, documents obtained by The Canadian Press say the Treasury Board Secretariat and Finance departments were notified of "harmful activity" on 24 Jan by the agency that oversees communications security in Canada.
- On 21 Oct 11, media reported that the Chief of CSEC, Mr. John Adams, is expected to step down from his post in early 2012. Media reported that no replacement has been named at this time.
- On 31 Oct 11, media reported on the relationship between CSE and CSIS. Coverage noted that CSIS works very closely with CSE and that while CSE's intelligence provides CSIS with investigative leads, information collected in the course of CSIS investigations enhances CSE's ability to respond to cyber-threats.

- On 19 Dec 11, media reported that the new Communications Security Establishment Canada's (CSEC) headquarters will have filtered drinking fountains that will cost \$200 each. The article also noted that the Union of National Defence Employees agrees that CSEC needs a new building, but has raised questions about why the complex has to be so elaborate even as DND is facing cuts.

Responsible Principal(s): CSEC

Contact: Adrian Simpson, Spokesperson, CSEC, 613-949-2218

Sarah Pacey (D Parl A 2-2), 995-8331

19 December 2011